CALEA Implementation Unit
14800 Conference Center Drive, Suite 300
Chantilly, Virginia 20151

December 18, 2003

Marlene H. Dortch, Secretary
Federal Communications Commission
445 12th Street, SW
Washington, D.C. 20554

Re: Notice of *Ex Parte* Presentation
        (CC Docket Nos. 02-33, 95-20 and 98-10; CS Docket No. 02-52)

Dear Ms. Dortch:

Pursuant to Section 1.1206(b) of the Commission's Rules, 47 C.F.R. § 1.1206(b), the Federal Bureau of Investigation ("FBI") hereby submits notice of an *ex parte* meeting on December 17, 2003.

The FBI representative who attended the meeting was Martin J. King of the FBI's Office of General Counsel. Also participating in the meeting on behalf of the FBI were Kenneth Coon, Joel Margolis, Kevin Minsky, and Valerie Furman, consultants to the FBI's CALEA Implementation Unit.

The Commission staff members who attended the meeting were Ed Thomas, Julius Knapp, Geraldine Matise, Jerome Stanshine, Jeffrey Goldthorp, and Jamison Prime of the Office of Engineering and Technology; David Ward, Cathy Zima, and Michael Goldstein of the Wireline Competition Bureau; Stanley Wiggins, Eugenie Barton, and Patrick Forster of the Wireless Telecommunications Bureau; and Dan Emrick of the Enforcement Bureau's Office of Homeland Security.

The purpose of the meeting was to discuss the Communications Assistance for Law Enforcement Act ("CALEA"), 47 C.F.R. § 1001 *et seq.*, in the context of the above-referenced dockets.[1] Specifically, the FBI explained the technical reasons why law enforcement requires Internet access service to be subject to CALEA.

Without CALEA, lawful electronic surveillance of Internet access service is unduly burdensome, inefficient, and unreliable. With CALEA, the above problems can be solved, thus permitting law enforcement to fulfill court orders for lawful electronic surveillance on Internet access networks. The FBI further explained that it takes a service-by-service evaluative approach to the process of developing CALEA standards for lawful surveillance of Internet access -- *i.e.*, the same approach used by industry to develop CALEA standards for other services. A more detailed description of the matters discussed at the meeting is attached hereto as Exhibit A.

Respectfully submitted,
THE FEDERAL BUREAU OF INVESTIGATION

_____/s/ Martin J. King_____
Martin J. King
Office of the General Counsel
Federal Bureau of Investigation
14800 Conference Center Drive, Suite 300
Chantilly, Virginia 20151
(703) 814-4700

Enclosure

---

[1]   *See In the Matter of Appropriate Framework for Broadband Access to the Internet Over Wireline Facilities; Universal Service Obligations of Broadband Providers; Computer III Further Remand Proceedings: Bell Operating Company Provision of Enhanced Services; 1998 Biennial Regulatory Review – Review of Computer III and ONA Safeguards and Requirements*, Notice of Proposed Rulemaking, 17 FCC Rcd 3019 (2002); *In the Matter of Inquiry Concerning High-Speed Access to the Internet Over Cable and Other Facilities; Internet Over Cable Declaratory Ruling; Appropriate Regulatory Treatment for Broadband Access to the Internet Over Cable Facilities*, Declaratory Ruling and Notice of Proposed Rulemaking, 17 FCC Rcd 4798 (2002).

cc (via e-mail): Ed Thomas, Julius Knapp, Geraldine Matise, Jerome Stanshine, Jeffrey Goldthrop, Jamison Prime, David Ward, Cathy Zima, Michael Goldstein, Stanley Wiggins, Eugenie Barton, Patrick Forster, and Dan Emrick

EXHIBIT A

I. Why Carrier-based Capabilities for Interception of Public IP Network Access Service (PIPNAS) are needed

    A. Resources and Expertise Required for Interception
- Without CALEA
  - Resources required for each PIPNAS intercept far exceed traditional telephony intercepts
- With CALEA
  - Carrier assistance provides a more efficient division of labor
  - Standards help identify the appropriate capabilities for carriers to support in a given architecture and service
  - Standardized solutions provide a consistent set of information
  - Carrier-assisted, standardized solutions provide higher reliability, performance, and quality
  - Carrier-assisted, standardized solutions expedite the initiation of an intercept

    B. Isolation and Authentication of Intercepted Communications
- Without CALEA
  - Law Enforcement ad-hoc solutions are positioned to intercept a stream of data containing the traffic of many users
- With CALEA
  - Carrier-based capability that isolates and authenticates the subject's communications for delivery to law enforcement would only provide reasonably available communications and call-identifying information (and does not provide to law enforcement the communications of users who are not surveillance subjects)

    C. Impacts of Network-Based Services on Interception
- Without carrier assistance, law enforcement will not have access to network-based capabilities outside subject's full packet stream

II. Capabilities Requested

    A. CALEA Surveillance of Packet-Based Communications
- Delivered surveillance information should be service driven, not technology driven
  - Surveillances are focused on service events that occur (e.g., communication origination, communication failure)
  - Underlying technologies only impact the format of surveillance information (e.g., calling and called party address formats)
- Packet is a technology over which services are offered, not a service in and of itself

    B. PIPNAS Service Specific Document (SSD) focuses on *surveillance events* and information for surveillance events
- End-user actions and related signals associated with PIPNAS services that are CII or generate CII

C.   Information Requested for PIPNAS Interception
- Access Session Related Events
- Mobility Related Events
- Service/Subscription Related Events
- Service Change (Signaled) Events
- Packet Transport Related Events
- Surveillance Status Related (Objectives) Events